no $a_i a_j$ terms - the (*S*) equations are n equations of degree one in the a_i variables when the a'_i variables are fixed).

B1

Step 3: Let A be the element of K^{2n} defined by $A = (a_1,\ldots,a_n, a'_1,\ldots,a'_n)$. A is transformed into x such that $x = s^{-1}(A)$, where s is the secret, bijective and affine function from K^{2n} to K^{2n}.--

In the claims:

Kindly add the following new claims:

--37. A method according to claim 1 and wherein said supplying comprises obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$, $\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

B2

38. A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

39. A method according to claim 37 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.

40. Apparatus according to claim 18 and wherein the set S1 is obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized in that all coefficients of components involving orders higher than 1 of any of the n "oil" variables $a_1,\ldots,a_n$ and coefficients of components involving multiplication of two or more of the n "oil" variables $a_1,\ldots,a_n$ in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k), \ldots, P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

41. Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy one of the following conditions:

(a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, where K is a finite field over which the sets S1, S2 and S3 are provided,

(b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and less than or equal to $n^3/6$, and

(c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and less than or equal to n^4.

42. Apparatus according to claim 40 and wherein the set S2 comprises a set S of k polynomial functions of a UOV scheme, and the number v of "vinegar" variables is selected to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2, where K is a finite field over which the sets S1, S2 and S3 are provided and q is the number of elements of K.--